IN THE SPECIFICATION:

Please amend the paragraph beginning on page 8, line 11 as follows:

--Focusing now on the functions of LIM card **104**, in the illustrated embodiment, LIM **104** includes a number of sub-components including an SS7 MTP level 1 and 2 process **110**, an I/O buffer or queue **112**, a gateway screening (GWS) process **114**, an SS7 MTP level 3 discrimination process **116**, a distribution process **118**, and a routing process **120**. MTP level 1 and 2 process **110** provides the facilities necessary to send and receive digital data over a particular physical medium. MTP level 1 and 2 process **110** also performs error detection, error correction and sequenced delivery of SS7 message packets from the SS7 network. I/O queue **112** provides for temporary buffering of incoming and outgoing signaling message packets. GWS process **114** examines received message packets and determines whether the messages should be allowed into SG **100** for processing and/or routing. Gateway screening may include examining the destination point code of the received MSU to determine whether the MSU is to be allowed into a network for which SG **100** routes messages. While this level of screening may be effective in screening message from and to specific nodes, it fails when the point codes of the nodes from which or to which it is desirable to screen messages are not known. Since point codes of source and destination network nodes may not be known to transit networks, gateway screening alone may not be sufficient for screening MAP messages in a transit network.--

Please amend the paragraph beginning on page 15, line 15 as follows:

--If the CgPA or CdPA matches one of the screening criteria, control proceeds to step ~~**ST10**~~ **ST11** where MAP screening process **126** performs MAP screening on the message by examining the opcode field in the MAP portion of the message to determine the MAP message type and whether the message is of a type targeted for screening. In step **ST12**, if it is determined that the MAP message type is of a type targeted for screening, MAP screening process **128** applies the MAP/SCCP transit network screening rule. Table 1 shown below illustrates exemplary MAP/SCCP transit network screening rules that may be applied.--

Please amend the paragraph beginning on page 16, line 3 as follows:

--In Table 1, each row corresponds to a MAP/SCCP screening rule. In the first row in Table 1, called party address ranges from 9194938000 to 9194939999 may represent a destination network for MAP messages. This destination network may ~~determine~~ decide that anytime interrogation messages from any source network should be prohibited. Accordingly, the CgPA field may be set to a wildcard value. Thus, the first row in Table 1 represents a MAP/SCCP screening rule based on SCCP CdPA and MAP message type. The screening action to be performed when a message that matches the screening criteria is received is BLOCK, indicating that the message should not be allowed into the network.--

Please amend the paragraph beginning on page 16, line 13 as follows:

--The second row in Table 1 indicates that MAP location update messages originating from [[an]] a network represented by calling party address ranges 919749000-9197499999 to a network represented by called party address ranges 9193800000-9193809999 should be recorded. In this situation, the transit network may agree to route traffic associated with roaming subscribers between the two networks while charging a fee for such routing. In order to charge the proper fee, the owner of the transit network must record some or all of the message to create a billing record and charge the appropriate fee. Accordingly, the screening action for this example is RECORD, indicating that all or part of the message should be recorded.--

Please amend the paragraph beginning on page 22, line 15 as follows:

--Figure 5 is a network diagram illustrating another example of messages that may be blocked by MAP screening module **108** according to an embodiment of the present invention. In Figure [[3]] 5, it is assumed that a subscriber **500** of network A **402** has roamed into a service area of network C **406**. It is also assumed that network A **402** does not have a roaming agreement with network C **406**. In this situation, it may be desirable for network A **402** to be able to block location update messages originating from its subscribers roaming in network C **406** to avoid unnecessary processing by network A's HLR **502**.--